PLAINTIFFS' MOTIONS IN LIMINE 1 TO PRECLUDE GOOGLE FROM RELYING ON NON-PUBLIC SOURCE CODE AT TRIAL

Exhibit 4

Redacted Version of Document Sought to be Sealed

quinn emanuel trial lawyers | san francisco
50 California St., 22nd Floor, San Francisco, California 94111 | TEL (415) 875-6600 | FAX (415) 875-6700

WRITER'S DIRECT DIAL NO.
(415) 875-6426

WRITER'S INTERNET ADDRESS
jonathantse@quinnemanuel.com

May 25, 2021

VIA E-MAIL

Alexander Frawley
Susman Godfrey L.L.P.
1201 Avenue of the Americas, 22nd Floor
New York, NY 10015-6023

Re: *Brown, et al. v. Google LLC* – U.S. District Court, Northern District of California, San Jose Division: Case No. 5:20-cv-03664-LHK-SVK

Dear Counsel,

I write in response to your April 30, 2021 letter seeking non-public Google source code in response to Plaintiffs' Requests for Production ("RFP") Nos. 47, 51, 54, 58, 62, 66, 69, and 90.

To justify its production, Plaintiffs must establish that Google's non-public source code is relevant and necessary to this case. *See, e.g.*, *In re Apple and AT&T Antitrust Litig.*, 2010 WL 1240295, at *2, *3 (N.D. Cal. Mar. 26, 2010) (rejecting plaintiffs' request for source code discovery because "Plaintiffs only speculate that the . . . source code may be relevant" and therefore "have not met their burden and have not established that the . . . source code sought is *relevant* and *necessary*") (emphasis added). The Federal Circuit and other courts have held that source code production is not required in accordance with Federal Rule of Civil Procedure 26(b)(1) where the requesting party has not shown that all the source code was "needed or relevant" in the case. *See, e.g.*, *Drone Techs., Inc. v. Parrot S.A.*, 838 F.3d 1283, 1300 (Fed. Cir. 2016) (finding that the district court abused its discretion in ordering source code to be produced); *3rd Eye Surveillance, LLC v. United States*, 143 Fed. Cl. 103, 111-12 (2019) (denying a motion to compel source code after finding that plaintiffs have neither "demonstrated with any specificity that they require access to defendants' source code" nor "properly explained why existing discovery, such as manuals, technical documents, and other non-source code information, is insufficient for them" to support their allegations); *Campbell v. Facebook Inc.*, 2016 WL 7888026, at *2 (N.D. Cal. Oct. 4, 2016) (denying plaintiffs' motion to compel inspection of Facebook's "highly proprietary source code," finding it "unreasonable and disproportionate in light of the narrow issues . . . in the case"); *Abarca Health, LLC v. PharmPix Corp.*, 806 F. Supp. 2d 483, 491 (D.P.R. 2011) (denying request for production of source code after

determining that the source code's relevance was "questionable" and "even if relevant, compelling disclosure of the [s]ource [c]ode . . .would be unnecessary and would merely burden defendants without commensurate benefit"); *Viacom Int'l Inc. v. Youtube Inc.*, 253 F.R.D. 256, 260-61 (S.D.N.Y. 2008) (finding that "speculative" reasons for inspecting confidential source code, *i.e.*, an "undisputed trade secret," that was the product of "50,000 man hours of engineering time and millions of dollars of research and development costs" was insufficient). And even if Plaintiffs are able to establish that Google's non-public source code is "relevant and necessary" to the case, "when alternatives are available, a court will not be justified in ordering disclosure." *Congoo, LLC v. Revcontent LLC*, 2017 WL 3584205, at *3 (D.N.J. Aug. 10, 2017) (collecting cases).

Plaintiffs have failed to make the requisite showing. Plaintiffs attempt to justify Google source code on the basis that they purportedly need to explore "1. Google's collection of private browsing data; 2. Google's association of private browsing data with other user data; and 3. Google's use of private browsing data." These bases are insufficient to support their disproportional and intrusive request for several reasons.

First, Plaintiffs have not identified any deficiency or missing information on any of these three topics in the myriad information Google has already made available. In particular, to date, Google has produced over 17,300 documents spanning over 51,000 pages, two declarations, and further testimony from two Google witnesses (Jesse Adkins whom Plaintiffs deposed, and David Monsees, who was deposed in *Calhoun* and the transcript produced in *Brown*). For example, at least RFP Nos. 51, 58, 62, and 66 request source code that are "embedded into the code of websites," which are already publicly available and which Google already produced. *See, e.g.* GOOG-BRWN-00024166, GOOG-BRWN-00046763, GOOG-BRWN-00010113.

Plaintiffs' purported need to "better understand Google's collection process and the precise data collected" (Pls.'s Apr. 30, 2021 Ltr. at 2-3) is too ill-defined and speculative to justify source code discovery, as courts have routinely found. *See, e.g.*, *Viacom*, 253 F.R.D. at 260 (finding that the requested source code's "secrecy is of enormous commercial value" and that "Google should not be made to place this vital asset in hazard merely to allay speculation"). To the extent there are any relevant and necessary functionalities not reflected in the public source code or in Google's productions, these can be addressed through other available means of discovery, such as document productions and depositions. *See, e.g.*, *3rd Eye Surveillance*, 143 Fed. Cl. at 111-12; *Congoo*, 2017 WL 3584205, at *3. Further, Google is willing to consider a stipulation establishing those functionalities as an undisputed fact. In any event, Plaintiffs have not identified any deficiencies to date.

Second, Plaintiffs' requests are overly broad, sweep in irrelevant information, and are therefore not proportional to the needs of the case. They seek the "complete, versioned, unobfuscated, and commented code" of the functionality at issue. In fact, the vast majority of the code requested—an undisputed highly sensitive trade secret—is irrelevant to Plaintiffs' narrow allegations that Google purportedly failed to adequately disclose to users that it would receive information when users who are logged out of their Google Account and in private browsing mode visit third-party websites that use Google Ad Manager or Google Analytics.

Plaintiffs' justifications in their letter demonstrate why source code has little relevance, if any, to their claims. They claim that "Google's collection of private browsing data allows Google to charge

advertisers and websites more for its services, including through targeted advertising, and that Google uses private browsing data to improve Google's own algorithms and technology, including Google search" is relevant to Plaintiffs' claims (common law claim, constitutional claim, and CDAFA claim), its damages, and Google's consent defense. But that explanation does nothing to justify the production of ***source code***. Those claims hinge on Google's disclosures to the putative class members and their expectation of privacy and do not require inspection of any source code. Further, personalization of search results or Google news content are not at issue in this litigation and far afield from Plaintiffs' allegations in this case. Any relevance to Google's non-public source code that Plaintiffs seek is heavily outweighed by the undue burden on Google and lack of proportionality to Plaintiffs' allegations in this case.

Plaintiffs' reliance on statements in the Court's order denying Google's motion to dismiss as support for its request for Google's non-public source code does not bear any weight. In its Order, the Court merely found that Plaintiffs had sufficiently pled allegations in the First Amended Complaint and made no determination whether their allegations are in fact true. Dkt. 113 at 20, 38. As an example, although Plaintiffs continue to allege that GStatic and Approved Pixels are used by Google "to associate private browsing data with user profiles," Google has already explained why that is not the case and why those services are not relevant. Mr. Adkins—who Plaintiffs deposed for close to seven hours—explained that "gfonts.gstatic.com does not [even] write cookies." Tr. 233:16. Plaintiffs are not entitled to discovery to highly sensitive source code based on far flung theories that are neither relevant nor necessary to Plaintiffs' allegations in this case.

Finally, Plaintiffs' purported need for source code indicating how Google receives private browsing data specifically rests on false premises. As an initial matter, Plaintiffs assume that Google distinguishes site visit data it receives according to whether the browser was in private browsing or not. In fact, Incognito mode is intentionally designed to prevent websites that use Google services (and Google) from determining whether a user is in private browsing or not. Because Google does not distinguish the data it receives according to whether a user is in private browsing mode, there is no specific source code for collecting private browsing data, associating private browsing data with other user data, or using private browsing data.

Further, Plaintiffs claim they seek source code related to "Google's storing, updating, refining, modifying, and profile of users and their data" and "Google internal and external facing applications, tools, and processes that use the information . . . to generate profiles on users and/or devices, including Google's Ad Personalization service" so that Plaintiffs can determine how Google "associates private browsing data with users and/or user's devices." Google, however, has stated consistently throughout this litigation that it does not link logged-out private browsing data to identified users. Indeed, even during the April 29 discovery hearing, Google unequivocally stated that Google does not tie the private browsing sessions at issue to Plaintiffs. Apr. 29, 2021 Hearing Tr. 25:22-26:5 ("We don't track people in private browsing mode. . . . [I]f you're in private browsing mode and you hop on and you do a search and you go to three websites, Google will know that some user or device went to those three websites and then you ended the session and then it's gone."). Therefore, the source code that Plaintiffs request (to determine how Google "associates private browsing data with users and/or user's devices") does not exist.

The Google documents that Plaintiffs cite do not support their contention that Google associates the data it receives—while logged-out users in private browsing mode browse websites that use Google

Ad Manager or Analytics—with user profiles. *See, e.g.*, GOOG-BRWN-26434 (describing that information provided by advertisers are encrypted differently in cookie spaces, such as Zwieback or Biscotti, to prevent disclosure of PII), -28925 (identifying other pseudonyms that are available field access types for logs, such as Android Logging, Analytics, and Pseudonymous, that Plaintiffs also have not shown are relevant to the issues in this case), -27290 (mentioning the [redacted] cookie in document about managing the rotation and access to cryptographic keys across Display Ads servers and makes no suggestion that the [redacted] cookie is relevant to Plaintiffs' allegations in this case), -29458 (listing various identifiers, many of which are irrelevant such as "youtube-visitor" or "assistant-item," but failing to justify why Plaintiffs are entitled *carte blanche* access to Google's database to simply explore data about the Named Plaintiffs and putative class members). But even if they did, Plaintiffs have not demonstrated why discovery through document production and depositions is insufficient to obtain the same information it seeks through inspection of Google's non-public source code. *See, e.g.*, *3rd Eye Surveillance*, 143 Fed. Cl. at 111-12; *Congoo*, 2017 WL 3584205, at *3.

Moreover, Plaintiffs' request to have "access to the Dremel search tool and other materials to explore the data Google has collected about the named Plaintiffs and their devices" is farfetched and not proportional. Plaintiffs do not require direct access to Google's internal tools to understand that those tools need inputs (authenticated or unauthenticated identifiers) to be searched. Google has, and will continue to, search its systems for the identifiers Plaintiffs have provided to Google. On May 12, we sent Plaintiffs a letter explaining how to preserve unauthenticated identifiers from their browsers. Have Plaintiffs taken these preservation steps? When will they provide Google with the preserved cookie values? Google cannot query its systems for data associated with unauthenticated identifiers without knowing the specific value of the unauthenticated identifier. Neither Google, nor anybody else, can search for data associated with unknown identifiers.

* * *

Google recognizes that there may be certain limited circumstances in which source code production may be appropriate and is willing to work with Plaintiffs to identify those circumstances, if any. We look forward to continuing to work with Plaintiffs to address and resolve these discovery issues.

Sincerely,

/s/ *Jonathan Tse*
Jonathan Tse